Council of the European Union

Brussels, 19 December 2017
(OR. en)

15861/17

JAI 1217
COSI 341
FRONT 517
ASIM 145
DAPIX 434
ENFOPOL 625
SIRIS 220
VISA 468
FAUXDOC 76
COPEN 423
CYBER 220
DATAPROTECT 223
CT 169
JAIEX 118
EF 347

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	14 December 2017
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2017) 779 final
Subject:	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL Twelfth progress report towards an effective and genuine Security Union

Delegations will find attached document COM(2017) 779 final.

Encl.: COM(2017) 779 final

EUROPEAN
COMMISSION

Strasbourg, 12.12.2017
COM(2017) 779 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL

Twelfth progress report towards an effective and genuine Security Union

I. INTRODUCTION

This is the twelfth monthly report on the progress made towards building an effective and genuine Security Union and covers developments under two main pillars: tackling terrorism and organised crime and the means that support them; and strengthening our defences and building resilience against those threats.

It is almost a year since the 19 December 2016 Berlin Christmas market attack which left twelve dead and fifty six injured and was perpetrated by an individual who used multiple identities to evade border and law enforcement authorities. This incident and other terrorist attacks committed by perpetrators who used multiple identities, such as the stabbing in Marseille in October 2017, not only highlighted the importance of effective information sharing between Member State authorities, but also the vital importance of the work begun by the Commission in spring 2016[1] to overcome the current shortcomings in EU information management which make it possible for an individual to appear in different EU databases using different identities. The legislative proposals for Regulations[2] on the interoperability of information systems, tabled as part of a package with this report, are designed to close down the space for terrorists and criminals to exploit the current gaps to perpetrate identity fraud, thereby better protecting the EU's external border, strengthening internal security and improving the management of migration.[3] The proposals represent a step-change not only in the way the EU manages information for security, border and migration management but also in making that data available to national authorities, to ensure that they have the information they need, when and where they need it. Given the central importance of these proposals to enhancing the effectiveness of border and law enforcement, the Commission now calls on the co-legislators to work on the legislative proposals on interoperability as a matter of the highest priority, and also to reach rapid agreement on the remaining legislative proposals on the table that relate to individual information systems to provide those in the front line with the information they need to do their jobs in keeping our citizens safe.

This report therefore focuses on the next steps towards stronger and smarter information systems for security, borders and migration management, to make the data architecture of EU information systems more effective and efficient, while at the same time ensuring full respect of data protection requirements.

This report also takes stock of a number of actions designed to maximise the benefits of existing information systems, covering legislative work as well as ongoing work to ensure their full implementation and better application of EU information systems. The October 2017 European Council took stock of the implementation of the Bratislava roadmap[4] and noted the significant progress made by the EU, in particular in the area of internal security, in four areas: intensified cooperation and information exchange, increased checks and interconnection of databases, development of a European Travel Information and Authorisation System (ETIAS) and systematic efforts against radicalisation. This report shows that further progress has been made in all these areas over the last two months.

---

1 COM(2016) 205 (6.4.2016).
2 COM(2017) 793 final and COM(2017) 794 final (12.12.2017).
3 COM(2017) 261 final (16.5.2017).
4 http://www.consilium.europa.eu/media/21597/bratislava-implementation-report.pdf

II. STRONGER AND SMARTER INFORMATION SYSTEMS FOR SECURITY, BORDER AND MIGRATION MANAGEMENT

Recent surveys show that EU citizens strongly support increased cross EU sharing of information in the fight against terrorism and organised crime.[5] The information provided by EU systems plays a vital role in helping national authorities to manage the external border, to fight crime and terrorism, and to curb irregular migration. To maximise this EU added value, the information provided by EU systems needs to be complete, accurate and reliable. The current picture is fragmented, complex and difficult to use.

To address these shortcomings[6], in line with the April 2016 Commission Communication, work has focused on three areas: maximising the benefits of existing information systems, developing new and complementary systems to plug gaps, and improving the interoperability of information systems.

1. Towards the interoperability of information systems

First, the proposed measures will help officers on the ground to **make best use of existing data**. A *European search portal* will provide a "one stop shop" – enabling the simultaneous search of multiple EU information systems[7] as well as the relevant Europol data and Interpol systems, in line with the users' access rights. This will give officers on the ground efficient, fast and seamless access to the data they need to do their job and remove the current complexity of deciding which database should be checked in any given situation.

Second, by using biometric data, the proposed measures will allow national authorities to **detect multiple identities and counter identity fraud**. A *shared biometric matching service* will enable the search and comparison of biometric data from several central systems[8], while a *common identity repository* will contain the shared biographical and biometric identity data of third-country nationals present in EU information systems.[9] Building on these two interoperability components, a *multiple-identity detector* will check whether data on a queried identity exists in more than one of the systems connected to it.[10] Whenever immigration and asylum officers record a person in EU information systems, or when police officers and border guards check a person against these systems, they will be informed if the person is already known under a different identity, or if the person uses multiple identities. This will close the current gaps and blind spots that terrorists and other criminals seek to exploit by hiding behind false or multiple identities.

---

5 See the Special Eurobarometer 464b Europeans' attitudes towards security published on 12 December 2017: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/1569.

6 COM(2016) 205 final (6.4.2016).

7 The Schengen Information System, Eurodac, the Visa Information System, the future Entry/Exit System, the proposed European Travel Information and Authorisation System and the proposed European Criminal Records Information System for third-country nationals.

8 The Schengen Information System, Eurodac, the Visa Information System, the future Entry/Exit System and the proposed European Criminal Records Information System for third-country nationals.

9 Eurodac, the Visa Information System, the future Entry/Exit System, the proposed European Travel Information and Authorisation System and the proposed European Criminal Records Information System for third-country nationals.

10 The Schengen Information System, Eurodac, the Visa Information System, the future Entry/Exit System, the proposed European Travel Information and Authorisation System and the proposed European Criminal Records Information System for third-country nationals.

Third, the proposed measures will enable police officers to carry out **rapid and effective identity checks within their territory**. During such checks, police officers will have access to the identity data of third-country nationals whose data is recorded in EU information systems, allow for the correct identification and detection of multiple identities. This will increase substantially the effectiveness of checks within Member States' territory, also in line with the Commission's recommendation on proportionate police checks and police cooperation in the Schengen area.[11]

To complement these interoperability components, the Commission also proposes to **facilitate and streamline law enforcement access** to non-law enforcement systems by introducing a new two-step data consultation approach. Already under current rules, law enforcement authorities can consult non-law enforcement information systems for the purpose of prevention, investigation, detection or prosecution of terrorism and other serious criminal offences. However, the respective systems are governed by different access conditions and safeguards, and some of the current rules hinder the efficiency of the legitimate use of the systems by these authorities. Under the new two-step data consultation approach, a law enforcement officer would first check in parallel all the systems storing their data in the *common identity repository* in order to know whether information on the searched person existed in any of the systems. To ensure data protection, only a "*hit/no-hit"* reply would be given. The officer would not have access to any data in any system but crucially would know if and where such data existed. In a second step, the officer would then be able to request full access to the information system(s) that generated hits, with an individual access request for each system concerned and in line with the respective rules established by each system concerned. Like today, the officer would need to justify the need to access the system, in line with that information system's access rights and purpose limitation principles, with subsequent full access remaining subject to prior authorisation by a designated authority and continuing to require a specific user ID and login. Once such a two-step data consultation approach applies, there will no longer be any need for a prior search in national databases and the launch of a prior search in the automated fingerprint identification system of other Member States under Decision 2008/615/JHA ('Prüm check').

The interoperability proposals **respect and promote fundamental rights and in particular the right to data protection**. With the new comprehensive framework for the protection of personal data in the EU in place and significant developments in technology and IT security, the principle of purpose limitation can be more easily implemented at the level of access and use to data stored, in full compliance with the Charter of Fundamental Rights and with recent European Court of Justice’s jurisprudence. The proposed measures will not lead to the interconnectivity of the individual systems. Each system will keep its specific purpose limitation, access rules and data retention rules. The proposed measures will also not lead to an increase in the collection of new data. They provide a targeted and intelligent way of using existing information held in EU systems to best effect.

The legislative proposals are the result of an **inclusive and transparent process** that started with the Commission Communication on Stronger and Smart Information Systems for Borders and Security of April 2016 which was followed up by a High-Level Expert Group[12]

[11] C(2017) 3349 final (12.5.2017).

[12] The Group was set up under Commission Decision 2016/C 257/03 (17.6.2016). It brought together experts from Member States and associated Schengen countries, and from the EU agencies eu-LISA, Europol, the European Asylum Support Office, the European Border and Coast Guard Agency and the Fundamental Rights Agency. The EU Counter-Terrorism Coordinator and the European Data Protection Supervisor

to address the legal, technical and operational challenges of different options to achieve interoperability.

The legislative proposals include detailed provisions for the **necessary changes to the legal instruments** that are currently stable texts as adopted by the co-legislators, namely the Schengen Borders Code, the Entry/Exit System Regulation, the legal instruments governing the Visa Information System. The other instruments covered[13] are currently under negotiation in the European Parliament and Council. For these instruments it is therefore not possible to set out the necessary amendments at this stage. The Commission will present such amendments for each for these instruments within two weeks after a political agreement on the respective draft Regulation will be reached. It calls on the co-legislators to reach swift agreement in the ongoing negotiations on these instruments.

2. Developing new and complementary actions to address gaps

In addition to the new proposals on interoperability set out above, it is vital that progress continues to be made on closing the current information gaps that the Commission identified in its April 2016 Communication in respect of third-country nationals visiting the Schengen area. The final texts of the Regulation on the **EU Entry/Exit System**[14] (EES) and the Regulation amending the Schengen Borders Code to align it to the EES[15] were adopted by the co-legislators at the end of November with entry into force by the end of 2017. Following this development of the system will start in 2018 to ensure that it is fully operational by 2020.

A further information gap – that of third country nationals who do not require a visa – was addressed in the Commission's November 2016 legislative proposal to establish a new large-scale IT system, the **European Travel Information and Authorisation System (ETIAS)**. The Council agreed its General Approach in June 2017 and the European Parliament's negotiating mandate was confirmed on 25 October 2017. Trilogue negotiations began the same day and continued on 16 November 2017 and 29 November 2017. The next political trilogue is scheduled to take place on 12 December 2017. The Commission calls on both co-legislators to reach a political agreement on the file by the end of 2017, in line with the European Council conclusions of December 2016 and the Joint Declaration.

3. Maximising the benefits of existing information systems

(a) Ongoing legislative work to strengthen existing information systems

As part of the Commission's efforts to maximise the potential of existing EU information systems, the Commission adopted three legislative proposals, in December 2016, to

---

participated as full members. Representatives of the Secretariat of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) and of the General Secretariat of the Council attended as observers. The final report of the Expert Group can be found at: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1. Its annexes include an executive summary of a report by the Fundamental Rights Agency as well as statements by the European Data Protection Supervisor and the EU Counter-Terrorism Coordinator.

13 The proposed Regulations on the European Travel Information and Authorisation System and the European Criminal Records Information System for third-country nationals, the Regulations on Eurodac, the Schengen Information System and eu-LISA, as well as those consequential amendments of the proposed Regulation on the European Travel Information and Authorisation System that concern the Regulation of the European Border and Coast Guard Agency.

14 Regulation 2017/2226 (30.11.2017).

15 Regulation 2017/2225 (30.11.2017).

strengthen the **Schengen Information System (SIS)**.[16] These include key measures to step up the fight against terrorism, such as introducing an obligation on Member States to create an alert in SIS if a person is sought in relation to a terrorist offence. Discussions in the European Parliament and the Council have also included the need to share information on terrorist offences in SIS with Europol, with amendments being proposed to make it possible for Europol and Member States to exchange supplementary information on SIS hits related to terrorism, and for Europol to cross-check information on newly created alerts and hits on such alerts against its databases and analytical work files. Negotiations between the European Parliament and the Council on these proposals began on 16 November 2017. Given the importance of these proposals, the Commission urges the co-legislators to reach an agreement on the proposals by early 2018.

In parallel, as planned since 2016, work continues to strengthen the SIS by introducing an **automated fingerprint identification system (AFIS)**. This will allow end users of SIS (such as police officers and border guards) to search the SIS on the basis of fingerprint data, allowing for reliable identification of people, including those travelling under false identities. Nine Member States have volunteered to take part in the first phase of the roll-out of the AFIS, expected to begin in March 2018. The full roll-out to all Member States using SIS is expected to be completed later that year.

As regards the legislative proposal to reinforce the **Eurodac**[17] system, trilogues are ongoing. Eurodac is one of the information systems that will be covered by the interoperability components, which is why it is important that the co-legislators reach swift agreement on this file. In the Communication setting out the Commission's contribution to the Leaders' meeting on a way forward on the external and the internal dimension of migration policy[18], the Commission calls for the proposal to be adopted by March 2018.

To further close down the space for terrorists and criminals, on 29 June 2017, the Commission presented a supplementary proposal to facilitate the exchange of criminal records of third-country nationals in the EU through the **European Criminal Records Information System (ECRIS)**.[19] The Justice and Home Affairs Council adopted, on 8 December 2017, a general approach on both the proposed Directive[20] and Regulation. The trilogue discussions between the co-legislators could start as soon as the European Parliament adopts its negotiating mandate on both ECRIS proposals. The Commission calls on both co-legislators to reach swift agreement on the proposals.

On 29 June 2017, the Commission adopted a proposal to revise the **mandate of the Agency for the operational management of large-scale IT systems in the area of freedom, security and justice**.[21] The Agency should be tasked with contributing to the development of interoperability between large-scale IT systems and with this in mind, the proposal is designed to review the Agency's establishing Regulation to take account of the recommendations stemming from the evaluation of the Agency, and to improve its functioning and enhance and strengthen its role to ensure that it can meet current challenges at EU level. It also aims at inserting changes deriving from policy, legal or factual developments

16 COM(2016) 881 final, 882 final and 883 final (21.12.2016).
17 COM(2016) 272 final (4.5.2016).
18 COM(2017) 820 final (7.12.2017).
19 COM(2017) 344 final (29.6.2017).
20 COM(2016) 7 final (19.1.2016).
21 COM(2017) 352 final (29.6.2017).

and in particular to reflect that new systems will be entrusted to the Agency. The European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) adopted its negotiating mandate on 7 December 2017, and the Council reached a general approach on the same day.

(b) Ensuring the full implementation of existing information systems

A key tool in the fight against terrorism and organised crime is the **Passenger Name Records (PNR) Directive**[22]. Although work continues across all Member States to ensure the full implementation of the Directive by the deadline of 25 May 2018, one year after the November 2016 PNR Implementation Plan[23] significant disparities remain between Member States' progress in setting up their national PNR systems. The transposition deadline is fast approaching. It is therefore crucial that these efforts intensify to deliver a successful conclusion by 25 May 2018. Of particular importance is the putting in place of the procedures and communication channels to allow national Passenger Information Units to share all relevant PNR data with the Passenger Information Units of other Member States and with Europol. This vital EU security tool will only be able to reach its full potential when all Member States have operational PNR systems in place and are able effectively to exchange data among themselves and with Europol. As of 15 November 2017, the picture is the following:

- Seven Member States already have both the legal and the technical capability to collect and process PNR data. However, most of these Member States still need to adjust their respective legal bases in order to be fully aligned with the requirements of the PNR Directive.
- Thirteen Member States are at an intermediary stage of implementation. Out of these, four have their Passenger Information Units (PIUs) established and equipped, but do not collect and process real PNR data because of the lack of a legal basis allowing the collection of personal data. The remaining nine Member States are in various stages of finalisation of the development or installation of the PIU and its technical solution to be used to process PNR data according to the requirements of the PNR Directive, while the engagement with air carriers is still ongoing. However, some of these nine Member States have already adopted legislation on PNR.
- Seven Member States are at a insufficiently advanced stage of the implementation process and still need to define the administrative architecture of their PIU, and/or submit the relevant legislation to their Parliaments, and/or start installing the technical solution to be used by the PIU, and/or launch the process to establish connectivity with air carriers.

The Commission continues to support Member States in their efforts to implement the Directive in a timely manner. The sixth meeting on the implementation of the PNR Directive was held on 3 October 2017 and allowed Member States' experts to update each other and the Commission on their progress in the implementation process and to share lessons learned, best practice and practical experience.

Financial assistance has been made available through the national programmes and EU actions under the Internal Security Fund – Police to support the setting up of functional PIUs

[22] Directive 2016/681 (27.4.2016).
[23] SWD(2016) 426 final (28.11.2016).

at national level and enable the exchange of PNR data between them in line with the PNR Directive[24].

Work also continues to ensure the full implementation of the **Prüm Decisions**[25] for the exchange of fingerprint data, DNA data and vehicle registration data. While most Member States have made progress in this regard, the Commission has had to use its infringement powers. The Commission sent Reasoned Opinions to Croatia, Ireland and Italy on 18 May 2017, and to Greece on 5 October 2017. In parallel, the Commission continues to support Member States by providing funding for implementation under the national programmes within ISF – Police. The Commission has provided an additional EUR 22 million to these national programmes for 2017 and this funding can be used for the implementation of Prüm.

(c) Support for better application of existing information systems

In addition to strengthening existing systems and ensuring their full implementation, the Commission is also working hard to support better application of existing information systems. Under the **Schengen evaluation mechanism**[26], on-site evaluations of the implementation of SIS take place in Member States every five years, carried out by Member State and European Commission experts in the field. In 2017, evaluation visits were carried out in Denmark, Iceland, Sweden, Portugal, Spain, Croatia, Norway and the UK. Any implementation issues identified during the evaluations are addressed through formal recommendations by the Council to the Member State concerned. Progress on past recommendations also forms part of the checks carried out by the evaluation teams during their on-site visits. Building on the findings of the Schengen evaluations carried out so far on the use of the Schengen Information System, the Commission will elaborate a set of **best practices and lessons learned** that provide added value across Member States to improve the application of existing information systems, for subsequent discussion with Member States.

To further improve information flows, Member States should make full use of technical solutions to improve the sharing of information with Europol. Automating the process of uploading data to the **Europol information system** for cross-checking purposes can significantly improve the sharing of relevant and up to date information with Europol and with other Member States. So-called 'data loaders' provide a technical tool for such automated uploading of data. Europol has developed such data loaders to allow Member States to improve their performance in uploading, updating and deleting data in Europol information system. These data loaders are already in use in several Member States.[27] In order to make Europol data available to a much wider group of police officers, an ongoing pilot project including five Member States (Spain, Estonia, Finland, Greece, Poland) focuses on the use of **QUEST**, a system interface that allows integrating automatic queries to Europol data from

---

[24] As announced in the Fifth progress report towards an effective and genuine Security Union, the Budgetary Authority reinforced the 2017 Union budget with EUR 70 million under the ISF-Police to support PNR-related actions during the period 2017-2020. These additional resources have been distributed as a top-up to Member States' national programmes according to the fund's allocation key. As regards Union actions, the "PIU.net" ongoing project, selected under an ISF-Police 2016 Call for Proposals, (with a maximum grant of EUR 3.78 million), aims to deliver a technical solution to facilitate the exchange of PNR data between Member States' PIUs. In November 2017 the Commission published an additional Call for Proposals, endowed with a total budget of EUR 1.5 million, for training, awareness raising and other capacity building actions targeted to the personnel working for the PIUs.

[25] Council Decisions 2008/615/JHA and 2008/616/JHA (23.6.2008).

[26] Council Regulation 1053/2013 (7.10.2013).

[27] For instance: Belgium, Finland, Poland, United Kingdom, and recently also by Czech Republic and Croatia.

national police information systems. This interface is expected to become operational in the beginning of 2018, after the validation by European Data Protection Service and operational tests by the Member States.

The Commission has contracted a study assessing the completeness and conformity of the measures of Member States to transpose the **Swedish framework decision**[28] that provides a common legal framework for the exchange of information between Member States' law enforcement authorities. The results are expected in the first quarter of 2018 and will be examined to see if new action is necessary. On 3 October 2017, the Commission issued a reasoned opinion to Luxembourg for non-communication of national measures taken to implement this decision.

III. IMPLEMENTATION OF OTHER PRIORITY FILES ON SECURITY

In addition to the work on closing information gaps and strengthening information systems, work has continued in a number of other areas of the Security Union.

1. Measures to improve protection and resilience against terrorism and crime

As a follow-up to the adoption of the Commission **Action Plan on the protection of public spaces**[29], the first meeting of the High Risk Security Network took place on 14-15 November 2017. The Spanish Guardia Civil Unit tasked with protection of high-risk places hosted this first conference at its headquarters in Logroño, Spain. This new network aims to support the development of new tactics to better protect high-risk public spaces. Moreover, the first meeting of the Operators' Forum will take place in Brussels on 20 December 2017, back-to-back with a dedicated thematic meeting on car rentals on 21 December 2017. Preparations have also started in regard to a meeting with mayors of European cities that will be held together with the Committee of the Regions in spring next year.

Responding to a heightened level of threat to transport, and specifically rail networks, some Member States have reinforced their security measures to protect rail transport. These measures have been carried out in a fragmented way, highlighting the need for improved coordination in the area of rail security. The Commission has therefore announced, in its Work Programme 2018, its intention to work towards further measures to improve **passenger railway security**.

In the area of research, the **Security Research** Event 2017 was co-organised by the European Commission and the Estonian Presidency in Tallinn on 14-15 November 2017. There was a wide acknowledgement that additional efforts are required to bridge the gap between research outputs, and effective products and services that can be used to tackle different security threats such as terrorism, cybercrime and natural disasters. Involving industry, academia, public authorities and practitioners in a co-creation process would help bring together supply-side (industry) and demand-side (end-users) to consolidate future requirements and agree on possible solutions that can have a practical impact and facilitate the work of security practitioners in the near future. The Commission will consider how to take these ideas forward.

---

[28] Council Framework Decision 2006/960 (18.12.2006).
[29] COM(2017) 612 final (18.10.2017).

2. Tackling the means that support terrorism

Discussions with co-legislators continued on the Commission proposal for amendments to the **4th Anti-money Laundering Directive**, which will help in the fight against terrorism financing. The Commission again calls on the co-legislators to finalise swiftly the legislative negotiations on this priority file and agree on a compromise that enhances the current set of Union rules on the prevention of money laundering and terrorist financing, including by enhancing transparency of beneficial ownership information.

In addition, the proposal for a **Directive to harmonise the definition and criminal sanctions of money laundering**[30] will help to overcome obstacles to cross-border cooperation in the fight against money laundering. A general approach was reached in Council on 8 June 2017. With the European Parliament adopting its position on 11 December 2017, the interinstitutional discussions will soon commence with a view to reaching agreement in the first half of 2018.

Work continues on possible measures to improve cross-border access by law enforcement authorities to relevant financial data that might provide necessary leads on terrorist activities, as announced in the Commission's Work Programme 2017. On 20 November 2017, the Commission organised a high-level stakeholder meeting with Member States and EU bodies to assess the need for **additional measures to facilitate cross border access to financial information for counter-terrorism purposes**. In this meeting, Member States noted that the various measures, whether existing, ongoing or planned, might provide the necessary tools and solutions, notably the **European Investigation Order**[31], the **Anti-Money Laundering Directive**[32] (including the proposal for amendments[33] currently under negotiation) and a forthcoming call for proposals to support Counter-Terrorism Financing projects[34].

The proposal for a revised 4th Anti-Money Laundering Directive envisages the mandatory establishment of **national centralised bank account registries and retrieval systems**, to which Financial Intelligence Units and anti-money laundering authorities would have access. The Commission is currently assessing the impact of relevant policy options with a view to proposing, in spring 2018, a Directive to grant law enforcement authorities and asset recovery offices access to the registries and data retrieval systems in their own Member State.

The Commission is also working on initiatives to improve the **cooperation between Financial Intelligence Units** as well as their cooperation with law enforcement authorities. This work should also be finalised in spring 2018. In parallel, and in view of preparing the necessary initiatives to facilitate cross-border access to financial data by law enforcement authorities, the Commission will continue to assess the necessity, technical feasibility and proportionality of any additional measures.

The Commission adopted today a report on the evaluation of Regulation 258/2012 on **export authorisation, and import and transit measures for firearms**. It concludes that the Regulation remains necessary but that its efficiency is limited by the lack of precision of some of its provisions, as well as by a complex interplay with other instruments of EU law. In order

30 COM(2016) 826 final (21.12.2016).
31 Directive 2014/41 (3.4. 2014).
32 Directive 2015/849 (20.5.2015).
33 COM(2016) 450 final (5.7.2016).
34 http://ec.europa.eu/research/participants/data/ref/other_eu_prog/other/home/call-fiche/isfp-call-fiche-2017-ag-terfin_en.pdf

to exchange views on these conclusions, the Commission will meet with national experts at the end of January 2018. It will also convene several meetings to move ahead on a number of challenges (seizure statistics, ballistics, cooperation with the Western Balkans countries).

On 18 October 2017, the Commission issued a **Recommendation on immediate steps to prevent misuse of explosives precursors**, urging Member States to urgently take a number of actions aiming to strengthen protection against the use of home-made explosives for terrorist purposes and supporting the objectives of Regulation 98/2013 on explosives precursors. A meeting of the Standing Committee on Precursors, on 12-13 December 2017, will take stock of the progress achieved by Member States in the implementation of the Recommendation. On 6 December 2017, the Commission decided to close the infringement procedure against France on the non-compliance with Regulation 98/2013, given that France informed the Commission of full implementation of the Regulation. In parallel, the Commission is **revising Regulation 98/2013** with a view to tightening the restrictions and controls on the sale, possession, introduction and use of explosives precursors, improving the capacity of economic operators and Member State competent and law enforcement authorities to detect and prevent instances of misuse, and increasing the degree of uniformity in the application of the Regulation across Member States. The impact assessment on the various options in revising the Regulation will be concluded in spring 2018.

3. Cybersecurity and criminal justice in the cyberspace

The European Council Conclusions of 19 October 2017[35] acknowledged the initiatives of the **Cybersecurity Package**.[36] On 20 November 2017, the Council adopted Conclusions on the Joint Communication to the European Parliament and the Council "*Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*".[37] An action plan to implement those Council Conclusions will be adopted by the General Affairs Council on 12 December 2017.

The discussions with the Council on the proposed **'Cybersecurity Act'** (covering the new ENISA mandate and the certification framework)[38] have started. The **legislative proposal on non-cash means of payments** has been presented to the European Parliament and Council and its examination is under way. The Commission urges that work in the European Parliament starts now that the Rapporteur was appointed on 13 November 2017. Regarding the implementation of the NIS Directive[39], a meeting of the Cooperation Group took place on 28 November. The Group adopted two of its deliverables concerning key aspects of the Directive: guidelines on the identification of operators of essential services[40] concerning good practices related to the criteria defining the criticality of an operator, and guidelines on security measures providing an overview of benchmarks for measures to be applied when securing network and information systems[41]. A third deliverable on notification requirements, setting out the circumstances in which Operators of Essential Services will be required to notify an incident, is expected to be adopted soon in written procedure. The Group

35 http://www.consilium.europa.eu/media/21620/19-euco-final-conclusions-en.pdf
36 https://ec.europa.eu/digital-single-market/en/policies/cybersecurity
37 JOIN(2017) 450 final (13.9.2017).
38 COM(2017) 477 final/2 (4.10.2017).
39 Directive (EU) 2016/1148 (6.7. 2016).
40 "Sharing of good practices related to the criteria defining the criticality of an operator pursuant to Article 5(2) of the directive by means of guidelines".
41 "Reference document on security measures for Operators of Essential Services".

has started engaging in talks concerning its first Work Programme (2018-2020), which should be adopted by February 2018.

The Commission committed in the 11th Security Union Progress Report[42] to assess the need for additional resources for Europol (in particular the European Cybercrime Centre, EC3) to enable EC3's support to Member States to address challenges related to **encryption in criminal investigations**. Considering the economies of scale achieved by providing an EU-level capability (compared to individual solutions at Member-State level), the Commission also took note of the need for further support in this area as called for by the Justice and Home Affairs Council on 7-8 December 2017. The assessment of the specific needs for additional resources is ongoing, and the Commission will report in the next Security Union Progress Report on the funds made available to this end. Enabling law-enforcement agencies from Member States to use tools provided by EC3 in a fast-changing field will allow the best return on investment and ensure that the European capabilities will remain up-to-date with the challenges, without prohibiting, limiting, or weakening encryption.

At the JHA Council meeting on 7-8 December 2017, Member States decided to continue discussions at expert level with a view to finding a common understanding of possible solutions on **data retention** in line with the Tele2 ruling of 21 December 2016. The Commission will continue to support Member States in this process. The Commission considers this process to be part of its own assessment on the ruling's implications and its ongoing work to finalise its guidance on the way forward on data retention as announced in the Commission Work Programme for 2018.

As previously announced, the Commission envisages bringing forward a legislative initiative on **electronic evidence** in early 2018 to facilitate law enforcement access to electronic evidence located in another country.

4. Countering radicalisation

Since the last Security Union Progress Report, the Commission has continued its work towards addressing radicalisation, both offline and online.

The **High-Level Expert Group on Radicalisation** set up in July 2017 continued its work at high pace towards its first interim report, which was agreed by the members of the Group on 24 November 2017. The preliminary findings and recommendations of the Group identify a number of priority topics and cross-cutting issues including radicalisation in prisons, local responses in a multi-agency setting, enhancing knowledge on radicalisation pathways, cooperation mechanisms and structures, education and social inclusion, as well as the external dimension of prevent work. The Commission will set out in the next Security Union progress report its views on these preliminary findings and recommendations.

The third Ministerial meeting of the **EU Internet Forum** took place on 6 December 2017, bringing together Member States, internet companies, Europol, academia and civil society representatives.[43] Progress under the Action Plan to combat terrorist content online was assessed, covering automated detection of terrorist content, improvements to the companies' 'database of hashes' to help stem the dissemination of terrorist content, enhanced referrals as well as empowering civil society to increase alternative narratives to terrorist propaganda.

[42] COM(2017) 608 final (18.10.2017).
[43] http://europa.eu/rapid/press-release_IP-17-5105_en.htm

Internet companies reported that the database of known terrorist content (the 'database of hashes'), announced in the 2016 EU Internet Forum and launched in spring 2017, is now operational and has so far gathered over 40,000 hashes of known terrorist videos and images. The potential of this tool should now be fully exploited, and data on the number of removals generated by the 'database of hashes' and speed of removals should be provided regularly to the EU Internet Forum members. The rate of manual referrals, such as from the EU Internet Referral Unit, also continues to increase and companies were urged to increase both the speed of removals and the regularity of reporting to the EU Internet Forum. Internet platforms reported that they are increasingly relying on automatic tools for the detection of terrorist content.[44] It is also important to increase the transparency, consistency and regularity of reporting results. All internet companies need to be part of this joint effort and share key information on content removals across platforms, prioritising outreach to and engagement with new and small companies that have not yet engaged in this.

The results of the EU Internet Forum will also inform the wider policy work on illegal content online, where the Commission announced that it will continue to promote cooperation with social media companies to detect and remove terrorist and other illegal content online, and if necessary will propose legislative measures on removing terrorist content.[45]

5. *External dimension*

On 7 December 2017, the Justice and Home Affairs Council gave the green light to the Commission to open negotiations with Canada on an Agreement between the EU and Canada for the transfer and use of Passenger Name Record (PNR) data to comply with Opinion 1/15 of the Court of Justice on the previously envisaged EU-Canada PNR Agreement. Formal negotiation will begin once Canada has obtained its own negotiating mandate.

As the Commission announced in the October Security Union Progress Report, the Commission is also adopting by the end of the year recommendations to the Council to authorise the opening of negotiations for agreements between the EU and Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey respectively on the **exchange of personal data between Europol and those countries' competent authorities** for fighting serious crime and terrorism. Such agreements will further strengthen Europol's capabilities to engage with these third countries for the purposes of preventing and combatting crimes falling within the scope of Europol's objectives.

As regards cooperation with international partners, the **EU and US held a Justice and Home Affairs Ministerial Meeting** on 17 November. The meeting focused on transatlantic cooperation on counterterrorism, on addressing cyber threats, and cooperation on drugs trafficking. On counterterrorism the discussion focused specifically on the importance of operational cooperation and effective information sharing. The two sides noted the importance of collecting, using, and sharing Passenger Name Record (PNR). The discussion also covered progress in the implementation of joint measures to address threats from terrorism to aviation and to raise the global baseline for aviation security. The EU and US referred to their actions on combating terrorism financing and money laundering, including

[44] Twitter reported that three quarters of the 300,000 accounts removed between January and June 2017 were deleted before posting content for the first time. According to YouTube, more than 150,000 videos have been removed since June 2017. Once aware of a piece of terrorist content, Facebook removes 83% of subsequently uploaded copies within one hour of upload.

[45] COM(2017) 650 final (24.10.2017).

common work and work within the Financial Action Task Force. Concerning the misuse of the internet for terrorist purposes, both agreed that work needed to be carried out in cooperation with multiple stakeholders, including the private sector and civil society. The next EU US Justice and Home Affairs Ministerial meeting will take place in Sofia in May 2018.

With regard to aviation security, the European Commission and other EU services are meeting regularly with Member States to agree on an **integrated approach to reinforce and prioritise capacity building efforts in third countries**. The proposed actions involve trainings and exercises on security culture, access control, screening procedures, certification of auditors, and others. Dedicated meetings for each of the assessed third countries are being organised, in order to design exact actions for each of those countries.

As a follow up to the Joint Declaration on the **NATO-EU strategic partnership**, the Council adopted on 5th December a second implementation report.[46] The report outlines the main areas where progress was made, including cybersecurity and countering hybrid threats. For the first time, the EU and NATO conducted a parallel and coordinated exercise (EU PACE17/CMX17) in September and October 2017 on the basis of a hybrid threat scenario. Together with the report, a set of 24 additional proposals was adopted to strengthen and deepen EU-NATO cooperation further. The new proposals cover all seven areas of cooperation identified in the Warsaw Joint Declaration: countering hybrid threats; broadening of operational cooperation, including at sea, and on migration; cyber security and defence; defence capabilities; defence industry and research; exercises; defence and security capacity building as well as political dialogue. Several of the proposals aim at strengthening cooperation in the areas of counter-terrorism. For instance, an informal workshop will be co-organised in the first half of 2018 in order to develop a shared understanding on how counter-terrorism efforts may benefit from defence capability development. Building on the experience and lessons learned in the exercise conducted in 2017, a plan will be developed for implementing parallel and coordinated exercises between the EU and NATO in 2019-2020. Moreover, starting in 2018, a set of common training and exercise modules will be rolled-out.

IV. CONCLUSION

This reports sets out a number of actions taken at EU level to step up the exchange of information to enhance internal security and better manage the external borders. The proposed Regulation on interoperability provides for a targeted and intelligent way of using existing data to best effect and integrating the principle of data protection by design. It constitutes a step-change in the way the EU manages data for security and external border, helping national authorities to better address transnational threats and detect terrorists who act across borders.

The next report on the progress made towards building an effective and genuine Security Union is planned to be adopted in January 2018.

[46] Responding to the tasking by the Ministers of both Organizations to report on a bi-annual basis, the first progress report on the implementation of the proposals was submitted to the respective Councils in June 2017. The second progress report covers the period July-December 2017.